New Jersey Domestic Security Preparedness Task Force

Infrastructure Advisory Committee

Chemical Group Security Assessment and Best Practices Report

Raymond Notaro, Huntsman Polyurethanes

Subcommittee
Leo Hurley, ExxonMobil Corporation
William Reiter, DuPont
Manny Ehrlich, ISP
Brian Bennett, Akzo Nobel Chemicals
Hal Bozarth, Chemistry Council of New Jersey

April 30, 2003

This report was prepared at the direction of the New Jersey Domestic Security Preparedness Task Force pursuant to its authority under the New Jersey Domestic Security Preparedness Act.

*** This document does not recommend a blanket mandate of any detailed procedures. Each company should evaluate what measures are appropriate based on economics, feasibility, and risk.**

TABLE OF CONTENTS

ASSESSMENT

The importance of security was recognized by the business of chemistry long before the terrorist events of September 11, 2001. Security permeates our industry and is a

vital part of our commitment to safety. Companies in the business of chemistry work hard to operate facilities in a manner that protects the health and safety of employees, the public, and the environment.

In recent years, companies have been developing and implementing security management practices. Earlier this year, a group of industry security experts convened to develop formal guidelines for implementing a site security management system to address concerns around physical, personnel and cyber-security. Guidelines exist within the industry that help individual facility managers make decisions on appropriate security measures based on risk.

The business of chemistry is unique in its approach to risk assessment because the security risks and needs of individual companies, and even those of individual facilities, can vary greatly from one to the next. With differing plant sizes, locations and chemicals produced and/or stored on-site, the variety of risks and security needs makes a blanket assessment of the industry's preparedness inherently difficult.

A multi-tiered, risk-based approach to assessment is the most effective and efficient way to evaluate, identify, and prioritize potential targets. A common type of assessment in the industry is a chemical hazards evaluation, in which hazards of a chemical are compared with the potential for exposure or potentially dangerous conditions. Chemical hazards evaluations are routinely performed in the chemical industry.

Companies in the business of chemistry also routinely perform a process hazard analysis, which analyzes the potential causes and consequences of fires, explosions, releases and major spills. The process hazard analysis focuses on equipment, instrumentation, human actions and external factors.

Another type of assessment conducted by the industry is a security risk assessment, which focuses on whether a company's security management program is adequate for protecting its assets. A risk assessment will take stock of the assets (employees, contractors, community residents, buildings, vehicles, equipment, storage tanks, raw materials, utilities, etc…) that need to be protected, the threats that may be posed against those assets, the likelihood and consequences of attacks against those assets and the company's response plans.

The business of chemistry recognizes that security is a top priority for the nation. Even with the many existing and proposed security modifications, the acts of September 11th have taught us that it is virtually impossible to guarantee every potential terrorist ploy has been identified. Responsible and conscientious operation of facilities is the best security prevention.

As an industry, we support companies conducting self-assessments of their security preparedness based on an evaluation of known or potential threats, volatility or quantity of hazardous chemicals on the premises or proximity to populated areas. We

*** This document does not recommend a blanket mandate of any detailed procedures. Each company should evaluate what measures are appropriate based on economics, feasibility, and risk.**

are opposed to excessive legislation that will mandate any requirements 'across-the-board,' without consideration for the resources and needs of individual companies.

The state can help the industry achieve our common goal of protecting employees, communities and the state's economy through several means detailed later in this document. These include a supplementation of on-site security at small facilities, tax breaks for security-related expenditures, financial support to conduct security surveys and financial support to implement universally agreed-upon best practices.

The business of chemistry is a critical and indispensable part of our nation's infrastructure. The business of chemistry is a nearly $30 billion industry in New Jersey, ranking the state second in the $460 billion-a-year enterprise throughout the United States. The industry makes thousands of products that make people's lives better, safer, and healthier—from medicines to medical equipment and space-age materials used by the military in stealth aircraft, aviation fuel, night vision equipment and satellite communications systems. Security in the business of chemistry is vital to the state's infrastructure and well being.

The American Chemistry Council issued a comprehensive Responsible Care Security Code on June 5, 2002. This code details the guiding principles to implement security measures at each of its' members facilities. The code includes the following elements: Leadership Commitment; Analysis of Threats; Vulnerabilities and Consequences; Implementation of Security Measures; Information and Cyber Security; Documentation; Training, Drills and Guidance; Communication, Dialogue and Information Exchange; Response to Security Threats; Response to Security Incidents; Audits; Third Party Verification; Management of Change; and Continuos Improvement.

The implementation of the American Chemistry Council Responsible Care Security Code is an acceptible alternative to the Best Practices as described in this "Chemical Group Security Assessment and Best Practices Report".

The following are ACC relevant documents that describe the Responsible Care Security Code.

- ACC Facility Security Prioritization Process

- Implementation guide for Responsible Care® Security Code of Management Practices

- Responsible Care® Security Code of Management Practices

The National Homeland Security Task Force developed a threat level advisory system. The Security Protective Measures Checklist for National Security Alert Levels, pages 13-18, was developed to provide guidelines to the business of chemistry members to implement security measures at each alert level. These guidelines should be implemented in a flexible manner to take into effect the specific security needs at each site.

CRITICALITY FACTORS AND RATING CATEGORIES

Criteria used to rate criticality, based on the severity of consequences:

- Effect on company personnel
- Effect on public in proximity to the facility
- Effect on company's finances
- Effect on company's operations
- Type of chemicals stored on premises
- Amount of chemicals stored on premises

Definition of rating categories:

Low

The consequence of the loss of this facility would have minimal or no effect on company personnel and an insignificant effect on the public, and the company's finances and operations.

Medium

The consequences of the loss of this facility would have a moderate effect on company personnel, as well as a moderate impact on the public's welfare, company's assets, revenue stream and disruption to operations.

High

The consequences of the loss of this facility would have a significant effect on company personnel and catastrophic impact on the public's welfare, company's assets, revenue stream and disruption to operations.

Best Security Practices

Topic #1: Communication with Public & Private Groups

Security Best Practice	Security Risk		
	High	**Medium**	**Low**
• Establish lines of communication by which government can pass along information on potential threats to the industry.	X	X	X
• Create an appropriate mechanism for threat assessment, communication and risk management	X	X	X
• Dialogue and partner with local, state, and federal agencies to understand potential threats	X	X	X
• Collaboration with state chemical associates	X	X	X
• Collaboration with CAP's around the state	X	X	X
• Collaboration with neighboring facilities to supply mutual aid in the event of an incident	X	X	X

Topic #2: Physical Security- Access Control

Security Best Practice	Security Risk		
	High	**Medium**	**Low**
• Post "No Trespassing", "Authorized Access Only" and 'All Vehicles & Visitors Are Subject To Search' signs	X	X	X
• To the extent feasible, employ normal surveillance by arranging reception, production and office space so unescorted visitors can be noticed easily	X	X	X
• Install appropriate locks on exterior and interior doors	X	X	X
• Keep closets and publicly accessible doors locked; set up key control system.	X	X	X
• Require visitor sign-in logs and escorts	X	X	X
• Install appropriate doors and security hinges.	X	X	
• Install secure windows with appropriate locks	X	X	
• Institute a system of employee and contractor photo ID	X	X	X
• Establish a system for determining which cars, trucks, rail cars, marine vessels and other vehicles may enter the site, through which gates, docks or other entrances and under what conditions.	X	X	
• Where appropriate, consider installing an electronic access control system that requires the use of key cards at main entrances and on other appropriate doors as an alternative to other measures that could provide the same security.	X	X	
• Consider electronic access control for entry to control centers, rack rooms, server rooms and other areas	X		

*** This document does not recommend a blanket mandate of any detailed procedures. Each company should evaluate what measures are appropriate based on economics, feasibility, and risk.**

Security Best Practice	Security Risk		
	High	**Medium**	**Low**
• Where appropriate, install a closed-circuit television system to monitor key areas of the facility as an alternative to other measures that could provide the same security	X	X	
• Where appropriate, employ motion sensors that mark the video recording and alert security staff when someone enters a restricted area	X		
• Require use of passes for removal of property from site	X		

Topic #3: Physical Security- Perimeter Protection

Security Best Practice	Security Risk		
	High	**Medium**	**Low**
• Appropriate fencing and exterior walls that make it difficult to enter the site	X	X	X
• Appropriate barriers that prevent vehicles from driving into the site at points other than official entrances	X	X	X
• Appropriate lighting that makes it easier for employees and passersby to observe and identify intruders	X	X	X
• Personnel gates or turnstiles	X		
• Well-kept landscaping that eliminates hiding places around perimeter	X	X	
• On-site security officers patrol perimeter and interior of facility at irregular intervals with no easily defined schedule	X		

*** This document does not recommend a blanket mandate of any detailed procedures. Each company should evaluate what measures are appropriate based on economics, feasibility, and risk.**

Topic #4: Backup Systems for Utilities

Security Best Practice	Security Risk		
	High	**Medium**	**Low**
• Appropriate back up or means of safe shut down in the event of a loss of electricity	X		
• Appropriate backup or means to provide basic service for emergency use in the event of a loss of communications	X		
• Appropriate backup or means to shut down or meet minimal needs in the event of a loss of water service	X		
• Appropriate backup or means of safe shut down in the event of a loss of natural gas service	X		
• Appropriate backup or means of safe shut down or meet minimal needs in the event of a loss of sewer service	X		
• Appropriate back up or means to provide nitrogen back up for tanks that could create an explosive hazard	X		

Topic #5: Training, Plans, Policies & Procedures

Security Best Practice	Security Risk		
	High	**Medium**	**Low**
• Train employees to challenge persons not wearing proper identification	X	X	X
• Company crisis management plan to support the response of the facility and community in the event of a security incident	X	X	X
• Termination program that maintains security upon employees resignation/ dismissal	X	X	
• Emergency response and crisis management plan	X	X	X
• Emergency response plan for civil disturbances	X		
• Policy that provides guidance on how to handle suspicious letters or packages	X	X	X
• Creation of bomb threat procedures	X	X	X
• Creation of an appropriate pre-employment screening policy	X	X	X
• Creation of a workplace violence policy	X	X	X
• Creation of an employee misconduct policy	X	X	X
• Creation of a general weapons policy	X	X	X
• Creation of a policy on drug and alcohol use	X	X	X
• Creation of unified security policies and procedures that address potential threats at specific facilities	X	X	X
• Creation of a security incident reporting and analysis policy	X	X	X
• Creation of a contractor training for what to do in case of emergency	X	X	X

*** This document does not recommend a blanket mandate of any detailed procedures. Each company should evaluate what measures are appropriate based on economics, feasibility, and risk.**

Security Best Practice	Security Risk		
	High	**Medium**	**Low**
• Formal plan for evaluating and continually improving security of a facility, understanding causes of security incidents and taking action to eliminate recurrence	X	X	X
• Periodic audits of security measures to assess procedures and determine whether modifications are needed	X	X	
• Provide for third party review of implementation of site adopted best practices. Third parties can be local police or fire officials, company security expert, state police or private security consultant.	X	X	

Topic #6: Transportation

Security Best Practice	Security Risk		
	High	**Medium**	**Low**
• Procedure for ensuring drivers who pick up or deliver hazardous materials are previously identified and trained properly	X	X	X
• Training of security personnel to keep detailed logs of deliveries & pick-ups, including driver info and destination	X	X	X
• Procedures to maximize the safety of materials and drivers during transit	X	X	X

Topic #7: Miscellaneous Issues

*** This document does not recommend a blanket mandate of any detailed procedures. Each company should evaluate what measures are appropriate based on economics, feasibility, and risk.**

Security Best Practice	Security Risk		
	High	**Medium**	**Low**
• Self-security audits/ reassessments for compliance	X	X	X
• Conduct Security Risk Assessments	X	X	X
• Periodic emergency response exercises, with local emergency personnel, testing the operability of the written security plan	X	X	
• Incident Reporting and Investigation and Analysis Program	X	X	X
• Security training for all employees on recognition of potential threats and site security procedures	X	X	X
• Identification of critical information readily available to employees, contractors and the public	X	X	X
• Firewalls, virus protection, encryption, user identification and passwords for computer access	X	X	X
• Ability to safely shut down process systems and equipment during incident or emergency	X	X	

SECURITY PROTECTIVE MEASURES CHECKLIST FOR NATIONAL SECURITY ALERT LEVELS

Threat Condition	Protective Measure	Start Date	End Date
Green	**Low Condition – Low Risk of Terrorist Attack**		
1	All facilities should know the identification of all employees and visitors and control access to critical facilities at all times. Contractors and visitors should not be allowed access to critical facilities unless the facility is satisfied as to their identity and there is a legitimate business purpose for their visit. Contractors and visitors must sign in and out of each Company facility using the existing Facility Sign In/Out Form.		
2	Ensure existing security measures are in place and functioning such as fencing, locks, camera surveillance, intruder alarms, and lighting.		
3a	Establish local, regional and system-wide threat and warning dissemination processes, emergency communications capability, and contact information with law enforcement.		
3b	Emergency communications should have redundancy in both hardware and means (phone, radio, e-mail, etc. as options) to contact law enforcement agencies.		
4	Develop terrorism and security awareness and provide information and educate employees on security standards and procedures.		
5	Advise all personnel at each facility to report the presence of unknown personnel, unidentified vehicles, vehicles operated out of the ordinary, abandoned parcels or packages, and other suspicious activities. Be alert to vehicles parked for an unusual length of time in or near a facility.		
6	Develop procedures for shutting down and evacuation of the facility. Facilities located near critical community assets should be especially vigilant.		
7	Incorporate security awareness and information into public education programs and notifications to emergency response organizations, e.g., landowner contacts, mail-outs, and local emergency planning committee advisories.		
8	Post “No Trespassing”, “No Weapons”, and “Authorized Access Only” signs along with signs stating that vehicles and visitors are subject to search.		
9	Periodically inspect perimeter fencing and repair all fence breakdowns.		
10	Conduct daily perimeter patrols of processing areas.		
11	Develop and implement hardware, software, and communications security for computer based operational systems.		

*** This document does not recommend a blanket mandate of any detailed procedures. Each company should evaluate what measures are appropriate based on economics, feasibility, and risk.**

Threat Condition	Protective Measure	Start Date	End Date
12	Instruct mail and package handlers to be on the alert for any questionable mail or package.		
13a	Ensure that a Company response can be mobilized. Review facility emergency and security plans and procedures annually.		
13b	Test security emergency communications procedures and protocols annually.		
14	Ensure that all delivery trucks have appropriate documentation (i.e., Bill of Lading, Material Shipping Order, delivery ticket, etc.)		
Blue	**Guarded Condition - General Risk of Terrorist Attack**		
15	Continue all Low (Green) level measures or introduce those that have not already been implemented.		
16a	Limit visitation and confirm that a visitor is expected and has a need to be at a critical facility.		
16b	All unknown visitors should be escorted while in the facility.		
17	Review all outstanding maintenance and capital project work that could affect the security of facilities. Ensure the work and involved personnel will not adversely affect security.		
18	Secure all access gates including rail entry and exit gates not staffed by a security officer (closed and locked or card entry access only).		
19	Conduct perimeter patrols of processing areas each shift.		
Yellow	**Elevated Condition – Significant Risk of Terrorist Attack**		
20	Continue all Low (Green) and Guarded (Blue) level measures or introduce those that have not already been implemented.		
21	Increase the frequency of warnings required by Low Condition (Green) and inform personnel of additional threat information as available. Implement procedures to provide periodic updates on security measures being implemented (daily, weekly or monthly as needed).		
22	Ensure that a Company response can be mobilized as appropriate for the increased security level. Review emergency communications procedures and back-up plans with all concerned.		
23	As appropriate, review with facility employees the operations plans, personnel safety, security details, and logistical requirements that pertain to implementing the Yellow (Elevated) security level.		
24	Inspect all mail and packages coming into a facility. Do not open suspicious packages. Review the United States Postal Services "Suspicious Mail Alert" and the "Bombs by Mail" publications at www.usps.com with all personnel involved in receiving mail and packages.		
25	Close & lock gates and barriers except those needed for immediate entry and egress at critical facilities. Inspect perimeter fences on a regular basis (during each shift or randomly as needed). Ensure that other security systems are functioning and are available.		

*** This document does not recommend a blanket mandate of any detailed procedures. Each company should evaluate what measures are appropriate based on economics, feasibility, and risk.**

Threat Condition	Protective Measure	Start Date	End Date
26	Secure all buildings and storage areas not in regular use. Increase frequency of inspections (hourly, during each shift or randomly as needed) and patrols within the facility including the interior of buildings and along the interior facility perimeter.		
27	Inspect on a more frequent basis the interior and exterior of all buildings and around all aboveground storage tanks, perimeter and other vulnerable areas in critical facilities.		
28	Direct that all personal, company, and contractor vehicles at critical facility sites are secured.		
29	Confirm availability of security resources (local police or professional security service) that can assist with 24/7 coverage of critical facilities.		
30	Check critical unmanned sites and remote valve sites at more frequent intervals for signs of unauthorized entry, suspicious packages, or unusual activities. Increase Right of Way (ROW) surveillance in critical areas.		
31	If applicable, check to ensure that all telephone, radio, and satellite communication systems are in place and they are operational.		
32	Instruct security guards to visually inspect the interior and exterior of all vehicles entering the main gate (a brief visual inspection by walking around the vehicle and looking inside the cab and cargo hold, no undercarriage inspections).		
33	All visitors must be verified with the host in order to authorize visitor entry.		
34	Increase perimeter patrols of all waterway entries onto the site.		
Orange	**High Condition – High Risk of Terrorist Attack**		
35	Continue all Low (Green), Guarded (Blue) and Elevated (Yellow) measures or introduce those that have not already been implemented.		
36	Caution employees not to talk with outsiders concerning their facility or its operations.		
37	Place all Emergency Response Team Members on standby.		
38	Cancel or delay all non-vital facility work conducted by contractors, or continuously monitor their work with company personnel.		
39	Reduce the number of access points for vehicles and personnel to minimum levels at critical facilities and randomly spot check the contents of vehicles at the access points.		
40	Move automobiles and other non-stationary items at least 30 yards from critical facilities, particularly buildings and sensitive areas, unless doing so would create a safety hazard or impede other security measures in place at the facility. Identify areas where explosive devices could be hidden.		
41	Secure 24/7 trained and knowledgeable security personnel (local police or a professional security service) to perform security functions to staff the impacted facilities; ensure that all security personnel have been briefed concerning policies governing the use		

Threat Condition	Protective Measure	Start Date	End Date
	of force and pursuit (as appropriate).		
42	Dedicate trained and knowledgeable security personnel (local police or professional security service) to assist with security duties at critical facilities to monitor personnel entering the facility, check vehicles entering the facility, and to patrol the area on a regular basis reporting to facility management as issues surface.		
43	H&S Manager to advise local police agencies that the alert level is at a High Condition (Orange) and advise them of the measures being employed. Request that police agencies increase the frequency of their patrols of the facility.		
44	Consult with local authorities about control of public roads and access points that might make the facility more vulnerable to terrorist attack if they were to remain open.		
45	Erect barriers to control direction of traffic flow and protect the impacted facility from an attack by a parked or moving vehicle - company vehicles may be used for this purpose.		
46	Limit access to critical facilities to those personnel who have a legitimate and verifiable need to enter the facility. Require positive identification of all personnel entering the facility - no exceptions.		
47	Check all security systems such as lighting and intruder alarms to ensure they are functioning. Modify lighting levels, as appropriate, to address changing security needs.		
48	Implement frequent inspections at critical facilities including the exterior and roof of all buildings and parking areas. Increase patrolling at night and ensure all vulnerable critical points are fully illuminated and secure.		
49	Schedule more frequent perimeter patrols and visits to remote valve sites, waterway entries, and other locations that are potentially impacted.		
50	Instruct employees working alone at remote locations or on the Right of Way (ROW) to check-in on a periodic basis.		
51	All visitors must be escorted at all times in the process area.		
52	Instruct security guards to conduct thorough internal and external inspections of all vehicles entering the process area including undercarriage inspections. Two classes of vehicles: trusted and other. For trusted vehicles (defined as employee and company owned), a brief visual inspection by walking around the vehicle and looking inside cab and cargo hold, no undercarriage inspections. For all other vehicles, conduct thorough internal and external inspections of all vehicles entering the process area including undercarriage inspections.		
53	Implement visual external inspection of railcars focusing on undercarriage and tops of cars. Inspections may be done as the cars arrive at the loading/unloading point.		

Threat Condition	Protective Measure	Start Date	End Date
Red	**Severe Condition – Severe Risk of Terrorist Attack**		
54	Continue all Low (Green), Guarded (Blue), Elevated (Yellow) and High (Orange) Condition measures or introduce those that have not already been implemented.		
55	Consider evacuating all non-essential personnel.		
56	Activate emergency response plans for the critical facilities.		
57	Reduce facility access points to the absolute minimum necessary for continued operation.		
58	Continuous security patrol activity at critical facilities to the maximum level sustainable. Increase perimeter patrols and inspections of facility.		
59	Augment security forces to ensure control of the facility and access to the facility and other potential target areas. Establish surveillance points and reporting criteria and procedures. Solicit assistance from the local police agencies in securing the facility and access. Cooperate with local police or other authorities if they direct security measures.		
60	Identify the owner of all vehicles at critical facilities and remove all vehicles, which are not identified.		
61	Only permit essential vehicles to enter the facility. Have trained and knowledgeable security personnel inspect all vehicles entering critical facilities including the cargo areas, undercarriage, glove boxes, and other areas where dangerous items could be concealed.		
62	Increase the frequency of call-ins from remote locations. Employees should not work alone in impacted areas.		
63	Consider shutting down impacted facilities and operations in accordance with contingency plans unless there is a compelling reason not to and evaluate prior to resuming operations.		
64	Implement business contingency and continuity plans as appropriate.		
65	No visitors (non-company) allowed in the plant.		
66	Mail is to be processed away from process or critical areas (including UPS, FedEx, etc.)		
67	Insure that all waterway entry points are continuously patrolled.		
68	Insure that all railcar entry and exit points are continually manned while open. All cars entering are stopped and thoroughly inspected at the entry point – under carriage, inside cargo holds (if safe to do so), tops of cars.		